UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Google account Sloanketler1@gmail.com See Attachment A	)	Case No. 20-757-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ❒ evidence of a crime;
- ❒ contraband, fruits of crime, or other items illegally possessed;
- ❒ property designed for use, intended for use, or used in committing a crime;
- ❒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Manufacture of child pornography, and attempt
18 U.S.C. 2252	Transportation, distribution, and possession of child pornography

The application is based on these facts:
See attached affidavit.

❒ Continued on the attached sheet.

❒ Delayed notice of _____ days ~~(give exact ending date if more than 30 days: _____)~~ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Kenneth Bellis
Applicant's signature

Kenneth Bellis, TFO, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/12/2020

/s/ Linda K. Caracappa
Judge's signature

City and state: Philadelphia, Pennsylvania

Linda K. Caracappa, U.S. Magistrate Judge
Printed name and title

Print Save As... Attach Reset

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your Affiant, Kenneth Bellis, Detective Sergeant with the Delaware County District Attorney's Office Criminal Investigation Division, being duly sworn, deposes and states the following:

1. Your Affiant, Detective Kenneth Bellis, employed by the Delaware County Criminal Investigation Division ("CID"), is also a member of a federal Task Force that directs its efforts in the area of Internet Crimes Against Children ("ICAC") and is comprised of federal, state, and local law enforcement. The ICAC Task Force is responsible for conducting undercover online investigations, responding to complaints regarding children sexually exploited via the Internet, conducting community education programs, and monitoring of the Internet for the trade of child pornography.

2. Your Affiant has been a law enforcement officer for approximately 29 years and currently serves as the commander of the Pennsylvania Internet Crimes Against Children Taskforce ("PA ICAC"). During this time, your Affiant investigated incidents of child abuse (including child sexual abuse) and child pornography. Your Affiant received training in the field of child sexual abuse as well as the use of the Internet by sexual offenders to seduce, entice, and gain access to children for the purposes of sexual exploitation.

3. Your Affiant also is assigned to and sworn as a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") since March of 2015. As an FBI TFO, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. Your Affiant conducted and participated in numerous investigations regarding child exploitation on the Internet, as well as other investigations involving the use of a computer

or computer systems. Your Affiant is familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. Your Affiant participated in investigations into numerous violations of state and federal criminal laws involving the sexual exploitation and abuse of minors, including manufacturing, possession, receipt, transmission, and distribution of child pornography, the use of the Internet to entice, seduce, and gain access to children, endangering the welfare of a child, terroristic threats, sexual assault, and conspiracy. In addition, your Affiant has prepared and executed numerous state and federal search warrants.

5. Your Affiant gained experience in conducting these investigations through training in classes and everyday work related to conducting these types of investigations. Your Affiant attended computer crime classes and participated in the execution of search warrants related to computer crimes, the majority of which have involved child exploitation and/or child pornography offenses.

6. The statements contained in this affidavit are based on your Affiant's experience and background as a police officer and detective, and information received from other law enforcement, including Officer Robert Graves from the Chester Police Department. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed to be necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251 and 2252 are located at Google Inc. and are located in the records associated with the Google account Sloanketler1@gmail.com, maintained by Google Inc. at the premises listed in Attachment A, for the items specified in Attachment B hereto.

LEGAL AUTHORITY

7. Title 18 U.S.C. § 2251(a) and (e) prohibit a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct, and any attempts to do so, for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live depiction of such conduct, if such person knows or has reason to know the visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

9. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Google. I request that Google be required to produce the electronic communications and other information identified in Attachments A and B hereto. Because Google is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do

that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden.

10. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Google pursuant to the search warrant. In reviewing these files, I will treat them in the same way as if I were searching a file cabinet for certain documents. E mails and chat logs will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

11. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

12. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Google to comply even though Google is not located in this district, because the Court has jurisdiction over the offense being investigated.

13. I also ask that the warrant direct Google to produce records and other information pertaining to this account. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth below to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

14. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

DEFINITIONS

15. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See Title 18 U.S.C. § 2256(5)).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. ' 2256(2)).

e. The "use" of a child to create pornography within the meaning of 18 U.S.C. § 2251 does not require the child be actively or consciously involved. A child is still "used" to manufacture child pornography, even when the child is unaware of what they are being subjected to. See United States v. Finley, 726 F.3d 483, 495 (3d Cir. 2013) (sleeping child can be "used" to manufacture child pornography. "It would be absurd to suppose that Congress intended the statute to protect children actively involved in sexually explicit conduct, but not protect children who are passively involved in sexually explicit conduct while sleeping, when they are considerably more vulnerable.") See also United States v. Levy, 594 F. Supp. 2d 427, 443 (S.D.N.Y. 2009), in which the district court held that, "As a matter both of common sense and public policy, the statute must be construed to protect all children, including those who are unaware of what they are doing or what they are being subjected to, whether because they are sleeping or under the influence of drugs or alcohol or simply because of their age."); United States v. Theis, 853 F.3d 1178 (10th Cir. 2017) (victim "used" to make child pornography within meaning of statute, despite the fact that she was unaware that she was being secretly taped while she showered and used the toilet).

f. "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Minor" means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).

h. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name B a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's

servers, and other information, which may be stored both in computer data format and in written or printed record format.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

j. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. § 2510(15)).

k. "Hash Value" is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, a hash value is generally considered to be a unique signature or fingerprint for a file.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

16. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

17. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer

system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

18. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

19. E-mail is a popular form of transmitting messages and or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

20. Internet-based e-mail is a service provided by an electronic communication service provider allowing individuals to send and receive e-mail from any Internet connected computer, regardless of their location or Internet service provider (ISP). Individuals utilizing Internet-based e-mail services access their accounts by "logging in" through the web-browser software installed on their computer, often by providing an account name and an associated password. Once the service provider's computers have determined the password is correct for the given account name, the individual "logged-in" can access any e-mail sent to their account, and or send e-mail to any other e-mail address accessible via the Internet.

21. Internet-based e-mail service providers reserve and or maintain computer disk storage space on their computer system, usually limited and closely regulated, for the use of the

service subscriber for the storage of e-mail communications with other parties, which include graphic files, programs, or other types of date stored in electronic form.

22. Internet-based e-mail service providers maintain records pertaining to the individuals who subscribe to their services. These records could include the account holder's name, address, date of birth, gender, occupation, and the Internet Protocol (IP) address used to establish the account and subsequent accesses to that account.

23. Any e-mail that is sent to an Internet-based e-mail subscriber is stored in the subscriber's "mail box" on the electronic communications service provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely. Electronic communications service providers can also perform backups of subscriber's email accounts as routine maintenance in case their servers become inoperable so the content in the subscriber's account is not lost.

24. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. Most Internet-based e-mail users have the option of saving a copy of a sent e-mail. Unless the sender of the e-mail specifically deletes the e-mail from the provider's server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained by the provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

25. Internet-based e-mail provider's typically offer services to their subscribers that allow them to store any electronic file (i.e. image files, text files, etc.) on servers maintained and or owned by the provider.

26. E-mails and other electronic files stored on an electronic communications service provider's server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the provider's server.

GOOGLE

27. Gmail is an Internet based electronic communications system operated by Google. It permits its users to communicate using e mail through their Gmail service, instant messages, text messages, and group messages through their Hangouts and Voice services, and other social networking type methods.

28. Google also allows its users to use other features such as Google Drive (a file storage and synchronization service developed by Google that allows users to store files on their servers, synchronize files across devices, and share files), Google Hangouts (a communication platform developed by Google which includes messaging, video chat, short message service (SMS) and voice over IP (VOIP) features), Google Duo (a video chat mobile app developed by Google that is advertised as a high-quality one-to-one video calling app for mobile platforms), and Google Photos (a photo sharing and storage service developed by Google that gives users free, unlimited storage of photos and videos).

29. These services permit users can upload files, to include photos and videos, to be stored in the "cloud" on Google servers and be accessed anywhere from any device as long as the user logs into his or her associated Google account. Users can automatically backup their photos and videos from their devices, such as a cell or smart phone, tablet, or computer, into their Google Drive or Photos storage. Users can also set up permissions to only allow themselves to have access to these files or share these files with other specific people.

30. Google also maintains records and history for each Google account. This includes, but is not limited to, data such as Bookmarks, Calendar appointments, Chrome Internet history and searches performed in the Chrome web browser, Location history where the account was accessed from and where device associated with the account was located, Map data to include locations visited and locations searched, and Voice and Audio recordings when using the users voice to perform searches or other functions on the device the account was accessed from.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

31. Your Affiant knows from training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that

do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, or exchange. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some

individuals may dispose of their collection of their sexually explicit materials or only seek them out when they want to view them in order to conceal their activities for fear of being caught.

g. Individuals who possess, receive, or produce child pornography often transfer these files between their different online accounts and electronic and storage devices, whether it is to conceal the files, to store them in one account or device versus another account or device, or to use in their communication with other child pornographers. I have investigated cases where individuals transfer child pornography files from one device, or account, or social media application to another. I have investigated cases where individuals store some or all of their child pornography collections in multiple electronic and storage devices.

SPECIFIC PROBABLE CAUSE

32. On March 30, 2020, a relative of a 10-year-old minor female victim made a report of sexual abuse with the Philadelphia Police Department. The incident jurisdiction was later determined to be Delaware County, Pennsylvania.

33. On April 3, 2020, the 10-year-old minor female child was interviewed at the Delaware County Child Advocacy Center ("CAC") regarding the alleged sexual abuse committed by her mother's boyfriend, identified by the child as "TJ," and later identified by the child's father as Edward Tyron Ross DOB: 10/6/1990. The name of the female child is known to investigators but is being withheld from this affidavit to protect her privacy. The child will be hereinafter referred to as V#1.

34. During the interview, V#1 described years' long sexual abuse committed by "TJ" on her beginning when she was five years old. V#1 stated that she was repeatedly forced to perform oral sex on "TJ" inside her house at 1006 Keystone Road, Chester, Delaware County, PA 19013. V#1 stated that the sexual contact occurred when she was alone with "TJ" after her

mother went to work. V#1 stated that she would try to hide in her closet or under her bed, but "TJ" would find her and make her perform the sex acts.

35. V#1 stated that "TJ" would take her to the bedroom he shared with her mother inside 1006 Keystone Road, where he would remove his clothes and lay on the bed. V#1 described seeing "TJ's" chest, legs, and "private part." V#1 further referred a "private part" as being a "bird" and "dick." V#1 said "TJ" would make her suck on his "private part" almost every day her mother was at work. V#1 said that if she did not do so, she would get punished by "TJ" and he would scream at her.

36. V#1 said she would use her hands and mouth to suck on "TJ's" private part. V#1 described the act by opening her mouth and making a motion with her hand simulating oral sex. V#1 stated that she would always wash her mouth out with water. V#1 said that she was not allowed to use her teeth and that "TJ" would yell at her if he felt teeth. V#1 said she would start to cry, and "TJ" would yell at her and send her to her room.

37. V#1 said that "white stuff" would gush out of a hole inside his private part. V#1 said that one time she started to get sleepy and the white stuff went into her mouth. "TJ" told V#1 it was her fault and to keep it in her mouth until she went into the bathroom to wash it out.

38. V#1 described "TJ's" position when she performed oral sex on him as laying down with his hands behind his head. V#1 also said sometimes "TJ" would be holding his phone looking at it and she could hear sounds coming from the phone.

39. V#1 described one occasion when "TJ" tried to put his "private part" inside her "butt." V#1 described having to lay down on her stomach when "TJ" tried to put his penis inside her "butt." V#1 said that "TJ" could not fit his private part inside her. V#1 said it was hurting her "butt" and she was crying while holding the covers. "TJ" said "you stupid girl it doesn't fit."

40. V#1 stated that she was not sure if "TJ" was taking pictures during the sex acts but remembers him holding his phone as if he were taking pictures or recording. V#1 described two different Samsung cellular telephones used by "TJ": She described his old phone as a silver colored Samsung, and his new phone as being a different color and a little thinner. V#1 believes that "TJ" uses a dark gray case and that he still has his old phone.

41. V#1 stated that she tried to write her mother a note that read "help me" using a pencil and red marker. On one occasion, "TJ" found the note and became upset. V#1 said she was punished. V#1 said she wrote five or six notes and would try to get them to her mother but that she doesn't believe her mother ever saw them.

42. On April 6, 2020, Officer Robert Graves from Chester Police Department obtained an arrest warrant charging Edward Ross with Pennsylvania violations of rape of a child, aggravated indecent assault of a child and related charges.

43. That same day, April 6, 2020, your Affiant met with Magisterial District Court Judge the Honorable Diane M. Holefelder who issued a search and seizure warrant authorizing the search or the person of Edward Tyson Ross and the residence located at 1006 Keystone Road, Chester, PA 19013.

44. At approximately 7:50 PM, detectives from the Delaware County Criminal Investigation Division and officers from the Chester Police Department executed the search and seizure warrant at 1006 Keystone Road, Chester, PA 19013.

45. Your Affiant encountered the victim's mother outside the property and informed her of the search warrant. She opened the front door and admitted detectives into the property. Your Affiant entered the property and announced, "police search warrant." After calling his name, Edward Ross exited the kitchen area and was taken into custody without incident.

46. Seized from Ross' pants pocket was one Samsung Galaxy S8 cellular telephone. During a search of Ross' bedroom and hallway closet, detectives seized a number of electronic items, including a Dell laptop, ANS cellular telephone - Model UL40, LG cellular telephone, ZTE cellular telephone - Model 242, and Memorex 1 GB flash drive.

47. During a forensic examination conducted by the Delaware County Criminal Investigation Division several different social media accounts were located on the Samsung Galaxy S8 cellular telephone seized from Ross. The examination determined that over 1,800 images had been uploaded to the Google Photos account sought to be searched by this warrant, identified as sloanketler1@gmail.com. At the time of the seizure of this phone, it had been set to automatically upload photographs to the Google Photo cloud storage account. The numeric file names of the 1,800 photos were identified on the phone, but the images themselves were not recovered (though the file extensions confirmed that these were photographs), meaning that the 1,800 images had been uploaded to his Google Photo cloud storage account and then later deleted from his phone.

48. In addition to the files that were uploaded to the Google Photos account, over 300 website names were identified on the cellphone's Google Chrome internet history. Many of the websites identified pornography videos related to father daughter sex. The names of the websites include:

- Making A Stepdaughter Sex Tape For Wife On Fathers Day -XVIDEOS.COM
- Daughter asks to suck my dick Search – XVIDEOS.COM
- Daughter blows dad while he phone calls her teacher – XVIDEO.COM
- Dad and daughter fuck after mom sleep – XVIDEOS.COM
- Dad Fires Cum Inside His Stepdaughter – XVIDEOS.COM

49. As stated in paragraph 32, a family member contacted police to report the sexual abuse by Ross, but Ross was not arrested at that time. The subsequent forensic examination of

the search history on the seized Samsung Galaxy S8 cellular telephone showed that on the day after Ross was reported to police, his phone was used to search Google, using the following terms:

- 3/31/2020 – "is there jail time for sexual abuse on a child
- 4/1/2020 – "where do I find the trash on my phone"
- 4/1/2020 – "if accused of child abuse and the claims are found unsubstantiated what happens"
- 4/1/2020 – "does child abuse have to be proven"
- 4/2/2020 – "statute of limitations pa"
- 4/5/2020 – "can u be arrested without evidence"
- 4/5/2020 – "can you be arrested on child abuse accusations"

50. An examination of an ANS cellular telephone recovered in Ross' bedroom determined that over 1,500 images had been uploaded to the Google Photos account sought to be searched as part of this search warrant, identified as sloanketler1@gmail.com. The numeric file names were identified on the phone, but the images themselves were not recovered, though the file extensions confirmed that these were photographs, meaning that the 1,500 images had been uploaded to his Google Photo cloud storage account and then deleted from the phone.

51. Similar to the website history on the Samsung Galaxy S8 cellular telephone, numerous pornography website names related to father-daughter sex were identified.

52. During the course of this investigation, your Affiant has continued to monitor Edward Ross' telephone calls at George Hill Correctional Facility. During one of his conversations between Ross and his mother, Ross confirmed his email account as the suspect account, sloankelter1@gmail.com.

53. Based on the information contained in this affidavit, your Affiant believes that Edward Ross used his Google account identified by email address sloankelter1@gmail.com to upload and store images that may depict the 10-year-old minor female victim being sexually

assaulted by Ross and engaged in sexually explicit conduct, in violation of federal law.

CONCLUSION

54. Based on the facts set forth in this affidavit, your Affiant submits that there is probable cause for this Court to believe that evidence of the violations of 18 U.S.C. § 2251 and 2252 will be found within the services provided through the Google account identified by, Sloanketler1@gmail.com.

55. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachments A and B.

56. In reviewing the files supplied by Google Inc, your Affiant and/or other law enforcement officers will treat them in the same way as if they were searching a file cabinet for certain documents. Emails and chat logs will be scanned quickly to determine if they are relevant to the search. If they are, they will be read. If investigators determine that they are not relevant, they will put them aside without further review full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or seized computer.

57. Google Inc. shall disclose responsive data, if any, by sending to Detective Sergeant Kenneth Bellis, 201 W. Front Street, Media, PA 19063, using the US Postal Service or another courier service, notwithstanding 18 U.S.C. § 2252, 2252A, or any other similar state or federal statute or code.

58. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachments A and B.

59. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation, may lead to the destruction of evidence. Accordingly, your Affiant requests that

the Court issue an Order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant and all attachments thereto, and all related docket entries be filed under seal until further order of this Court. A separate court order is attached.

Respectfully Submitted,

/s/ Kenneth Bellis
Kenneth Bellis
Task Force Officer, FBI
Det. Sgt., Criminal Investigation Division
Delaware County District Attorney's Office

SWORN and subscribed to
before me this 11th day
of May, 2020.

/s/ Linda K. Caracappa
HONORABLE LINDA K. CARACAPPA
United States Magistrate Judge

ATTACHMENT A

LOCATION TO BE SEARCHED:

All Google Inc. accounts and information, whether active, deleted, or disabled, associated with **Sloanketler1@gmail.com,** as outlined in Attachment B, stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheater Parkway, Mountain View, Northern District of California.

ATTACHMENT B1

Items to be Seized associated with the account Sloanketler1@gmail.com.

(to be produced by Google Inc.):

A) All account information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, SMS numbers, associated apps or services to include any Google Voice numbers assigned to the accounts and the true phone number associated with those Google Voice numbers, screen names, websites, and other personal identifiers; buddy lists, contacts, and address books;

B) All communications and messages made or received by the user to include e-mails (read, sent, deleted, draft, and unopened) whether in a mailbox, user created folders, or other storage locations, attachments, documents, graphics, and any other uploaded, saved, or associated files, including all private messages and text messages using Google Hangouts. If possible, any deleted email messages from account creation February 15, 2014;

C) All images, videos, and data stored in the users associated Google Photos, Google Hangouts, Google+, Google Cloud storage accounts;

D) All activity logs and IP logs, including all records of the IP addresses that logged into the accounts and logs showing user accounts or IP addresses with dates and times of when files were placed in the users associated Google Drive cloud storage accounts;

E) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

F) All privacy settings and other account settings or permissions granted to other users regarding the users Google Drive cloud storage accounts;

G) All records pertaining to communications between Google Inc. and any person regarding the user or the user's Gmail, Google Photos, Google+, Google Cloud, Google Voice, Google Hangouts or Google Drive accounts, including contacts with support services and records of actions taken;

H) Google Inc. shall disclose responsive data, if any, by sending to Detective Sergeant Kenneth Bellis, 201 W. Front Street, Media, PA 19063 using the US Postal Service or another courier service, notwithstanding 18 U.S.C. §§ 2252, 2252A, or any other similar federal or state statute or code.

I) Preserved data requested on April 8, 2020 by Detective Sergeant Kenneth Bellis Delaware County Criminal Investigation Division, **Google reference number 3654494**.

J) The data listed above in paragraphs A through K shall be produced by Google regardless of where it may be stored.

Attachment B2

(Items Associated with the Account Sloanketler1@gmail.com)

To be Seized by Law Enforcement:

Evidence of the violations of 18 U.S.C. § 2251 and 2252, as follows:

A. All files, documents, communications, images, videos, logs, and contacts associated with the Google account **Sloanketler1@gmail.com**, related to visual depictions of minors engaging in sexually explicit conduct, in violation of Title 18 U.S.C. Sections 2251 and 2252, along with any evidence that would tend to show the true identities of the persons committing these offenses, the identities of the persons depicted in the images, videos, or other files, or the identities of the persons distributing or receiving the images, videos, or other files.

B. All activity logs and IP logs, including all records of the IP addresses that logged into the account.

C. All account information, including:

a. All account information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, services and apps used, downloaded, or purchased, and other personal identifiers; buddy lists, contacts, and address books;

b. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

c. All privacy settings and other account settings;

d. All logs of devices and accompanying serial or model numbers and other identifying numbers to include dates of activation, registration, deactivation, or use;

e. All logs showing the location of the user;

f. All records pertaining to communications between Google LLC and any person regarding the user or the user's Google account, including contacts with support services and records of actions taken; and

g. All records that tend to show the true identity or location of the user of the account.